#3
8-22-03

BOX PATENT APPLICATION
Attorney Docket No. 24929

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Kenjiro UEDA, et al.

Serial No. Not Yet Assigned

Filed: March 8, 2002

For: **ENCRYPTION METHOD, DECRYPTION METHOD, AND RECORDING AND REPRODUCING APPARATUS**

REQUEST FOR PRIORITY UNDER 35 U.S.C. §119

Commissioner of Patents
Washington, D.C. 20231

Sir:

In the matter of the above-captioned application, notice is hereby given that the Applicant claims as priority date March 13, 2001, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2001-070011. Applicant also claims as priority date March 13, 2001, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2001-070012. Applicant further claims as priority date October 9, 2001, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2001-311114. Applicant further claims as priority date October 9, 2001, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2001-311117.

A Certified Copy of the corresponding applications are submitted herewith.

Respectfully submitted,

NATH & ASSOCIATES PLLC

Date: March 8, 2002

By: _____
Gary M. Nath
Registration No. 26,965
Customer No. 20529

NATH & ASSOCIATES PLLC
6TH Floor
1030 15th Street, N.W.
Washington, D.C. 20005
(202)-775-8383
GMN/ls (Priority)

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: March 13, 2001

Application Number: Patent Application No. 2001-070011

Applicant(s): VICTOR COMPANY OF JAPAN, LIMITED

December 28, 2001

Commissioner,
Japan Patent Office

Kozo Oikawa

Number of Certification: 2001-3112879

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　３月１３日

出願番号
Application Number: 特願２００１－０７００１１

出願人
Applicant(s): 日本ビクター株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年１２月２８日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３１１２８７９

【書類名】　特許願

【整理番号】　413000021

【提出日】　平成13年 3月13日

【あて先】　特許庁長官殿

【国際特許分類】　G11B 20/10

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　上田　健二朗

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　菅原　隆幸

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　猪羽　渉

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　日暮　誠司

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　黒岩　俊夫

【特許出願人】

【識別番号】　000004329

【氏名又は名称】　日本ビクター株式会社

【代表者】　守隨　武雄

【電話番号】　045-450-2423

【手数料の表示】

【予納台帳番号】　003654

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化方法

【特許請求の範囲】

【請求項１】

複数の単位ブロックが連続した情報を単位ブロック毎に暗号化する暗号化方法であって、

所定の単位ブロックを暗号化するための暗号鍵のシードは、前記所定の単位ブロック以外の一つ又は複数の単位ブロック、もしくは、前記所定の単位ブロック以外の一つ又は複数の単位ブロックを暗号化した情報に基づくものであることを特徴とする暗号化方法。

【請求項２】

再生順序のある複数の単位ブロックが連続した情報を単位ブロック毎に暗号化する暗号化方法であって、

所定の単位ブロックを暗号化するための暗号鍵のシードは、前記再生順序にて前記所定の単位ブロックより前の一つ又は複数の単位ブロック、もしくは、前記所定の単位ブロックより前の一つ又は複数の単位ブロックを暗号化した情報に基づくものであることを特徴とする暗号化方法。

【請求項３】

前記暗号鍵のシードが少なくとも２回以上連鎖していること特徴とする請求項２に記載の暗号化方法。

【請求項４】

前記連鎖が所定の回数でリセットされることを特徴とする請求項３に記載の暗号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、視聴制限のあるコンテンツを暗号化する際の暗号化方法に関するものである。

【０００２】

【従来の技術】

従来、映像や音声等のコンテンツは、ビデオテープやオーディオテープ等のテープ状記録媒体に記録されたり、ＣＤやＤＶＤ等のディスク状記録媒体に記録されたりしているが、これらの媒体に記録されたコンテンツをダビング等の行為によって不正にコピーされることが問題となっていた。

【０００３】

また、映像や音声等のコンテンツを記録する際にデジタル方式が採用されるようになり、上述した媒体への記録の他にデータ配信などによってもコンテンツが配布されるようになり、不正なコピーの防止はより重要になってきている。

【０００４】

次に、デジタルコンテンツデータに対するコピーの制限方法について説明する。近年、上述したように映像や音声のデジタル配信が普及してきたことにより、コンテンツの配信を行うコンテンツプロバイダによってデジタルコンテンツデータに「コピー禁止」や「一回コピー可」等の視聴制限をかけていた。このようなデジタルコンテンツデータでは、コンテンツの中にコピーガード信号を挿入することにより、コピーしようとしたときに、コピーした側のコンテンツの映像が乱れるといった効果をもたらしていた。

【０００５】

このような方法を採用したコピーガードの代表的なものとしてマクロビジョン方式（擬似シンクパルス方式、カラーストライプ方式）と呼ばれるものがある。これは、「コピー禁止」の制限がかかったコンテンツのアナログ信号の特定部分に一定の信号を組み込むことにより、このコンテンツを録画しても、録画機器が特定部分に組み込んだ信号を認識しながら録画するため、コピー後の画面を再生すると前述した信号の影響で画面が鑑賞に堪えないものとなってしまう方法である。また、この方式のコピーガードを採用したコンテンツをデジタル録画機器で録画しようとしても、録画機器がこの信号を認識して録画ができない仕組みとなっている。なお、デジタル放送のＰＰＶ（Pay Per View）番組にはこの方式が採用されている。

【０００６】

しかしながら、この方式のコピーガードでは画面を乱す信号を除去するだけで正常な状態でコピーできるため、このコピーガードを回避するための機器が市販されるようなことが行われてきた。

【０００７】

また、「一回コピー可」の制限がかかったコンテンツについてはコピー世代の管理をすることによって規定回数以上のコピーを防止してきた。この方法の代表的なものとしては、ＣＧＭＳ（Copy Generation Management System）と呼ばれるものがある。これは、コンテンツのデジタル信号の特定の箇所に特定のデジタル信号（１．コピー不可，２．コピー一世代のみ可，３．コピー無制限の三通り）を組み込み、この信号をデジタル録画機器が識別することにより、そのコンテンツに組み込まれる特定のデジタル信号が指示するようにコピーを制限する方法である。なお、ＭＤ（ミニディスク）のコピー世代管理にもＣＧＭＳ方式が採用されている。

【０００８】

しかしながら、ＣＧＭＳ方式もコピー世代に関するフラグを「コピー不可」のものから「コピー可能」のものに書き換えることによってコピーガードを解除することができた。

【０００９】

このようなことを踏まえて、ＤＶＤではデジタルコンテンツデータ自体に暗号をかけて媒体に記録するようにした。従って、データをそのまま取り出そうとしても暗号化がかかっているコンテンツを取り出すことになり、しかも、暗号鍵を取り出すことは困難であるので、実際に暗号化がかかっていないデジタル信号をコピーするのは難しくなった。

【００１０】

このような暗号化の方式の一つであるＤＥＳ（Data Encryption Standard）について説明する。ＤＥＳは平文(原文)、暗号文、暗号鍵共に６４ビットのサイズを持つブロック暗号である。ただし、暗号鍵は６４ビットのうち８ビットをパリティに使用しているため、実質的な暗号鍵の長さは５６ビットである。

【００１１】

ＤＥＳの基本構成を図１に示す。平文の隣り合った各ビットがほぼ３２ビット離れるようにビットの入れ替えが行われた後、１６段の同一の変換が繰り返し適用される。各段では、前段から入力される上位３２ビットのL_{n-1}と下位３２ビットのR_{n-1}をそれぞれひとまとまりとし、鍵生成部から入力される４８ビットの鍵K_nを用いて、それらをL_nとR_nとに変換して次段に出力する。そして、１６段目の出力のL_{16}とR_{16}とを入れ替えた後、IP^{-1}により各ビットを置換することで暗号文が出力される。一方、鍵は選択置換ＰＣ－１により８ビットのパリティビットが取り除かれると共に、残りの５６ビットの入れ替えが行われる。

【００１２】

その後、上位２８ビットのC_nと下位２８ビットのD_nをそれぞれひとまとまりとしてシフトを１６段繰り返しながら、各段毎に鍵K_nを作成する。図１に示したＤＥＳの基本単位である１６段の変換部は各段共に図２に示す構造となっており、前段からの入力（L_{n-1}，R_{n-1}）と次段の出力（L_n，R_n）は次の関係を満たす。

$L=R_{n-1}$，$R_n=L_{n-1}$ＥＸＯＲｆ（R_{n-1}，K_n）

ここでは、ＥＸＯＲは排他的論理和を示しており、関数ｆ（R_{n-1}，K_n）は、更に図３に示す構造を有している。

【００１３】

ｆ関数への入力R_{n-1}は３２ビットからなるが、拡大置換Ｅにより、４８ビットに拡大される。次に、その４８ビットとK_nとをビット単位で排他的論理和を取った後、６ビット単位の８個に分割され、それぞれがS_1～S_8のＳボックスに入力される。各Ｓボックスでは６ビットの入力が４ビットの出力に非線形変換される。最後に、その出力の４ビットを８個合わせた３２ビットが、置換Ｐによりビット位置が入れ替えられ、ｆ（R_{n-1}，K_n）の出力となる。

【００１４】

ＤＥＳの基本変換である式

$Ln=R_{n-1}$，$R_n=L_{n-1}$ＥＸＯＲｆ（R_{n-1}，K_n）

を解いて、（L_{n-1}，R_{n-1}）を（L_n，R_n）で表すと次式となる。

$R_{n-1}=L_n$，$L_{n-1}=R_n$ＥＸＯＲｆ（R_{n-1}，K_n）＝R_nＥＸＯＲｆ（L_n，K_n

)

これによって（R_n，L_n）から（R_{n-1}，L_{n-1}）を求める操作は、（L_{n-1}）から（L_n，R_n）を求める操作を同じ構造になっていることが分かる。この性質は、復号を暗号化と同じ変換で行うことができることを意味している。

【００１５】

【発明が解決しようとする課題】

しかしながら、例えばデジタル放送のＰＰＶ番組では「コピー禁止」の制限がかかっているため、そのコンテンツを一回だけ視聴することができるが、視聴者はＰＰＶ番組が放送されている決まった時間帯に見なければいけなかった。このように、「コピー禁止」のコンテンツについては、その著作権者がコンテンツの視聴を一回だけ許可する意図であったとしても、実際には視聴する時間帯を限定してしまうことになっていた。また、「コピー禁止」のコンテンツを記録媒体に記録して一回だけ視聴を許可する場合も、一回コンテンツを視聴したらコンテンツの再生を不可能とする方式が確立されていなかった。更に、これを実現するために、コンテンツを再生しながら見終わった部分のデータを消去するというのは処理が難しく実現が困難であった。例えば、パーソナルコンピュータ等でハードディスク上のデータを削除するのはファイルシステムのＦＡＴを消去しているだけなので、実際にデータを消去しているわけではなかった。

【００１６】

一方、「一回コピー可」のコンテンツは、例えばＶＴＲとＨＤＤ（ハードディスクドライブ）とを組み合わせた記録再生装置で記録する場合でも一回どちらかの媒体に記録したらそれ以上の記録は二回目のコピーとなってしまうためできなかった。従って、一度視聴した後に所望の番組だけを保存用の媒体に改めて記録することはできなかった。このように、「一回コピー可」のコンテンツについては、その著作権者がコンテンツが記録される媒体は一つに限定するという意図であったとしても、実際には一度記録したコンテンツを別の媒体に記録して元の記録媒体の記録部分を消去する、いわゆるコンテンツの移動が許可されていなかった。

【００１７】

また、暗号化に関しても、コンピュータの性能の向上によって暗号鍵を知ることが容易となった。そして、一つのコンテンツに固定の鍵を使用することは、その鍵を知ることができたらそのコンテンツ全てが解読されたことになり、その結果、デジタルコンテンツが違法にコピーされることが予想される。そこで、これを回避するために鍵を時間毎に変化させるという方法がある。これによってコンテンツの一部の暗号化に使用された鍵が知られても、コンテンツ全体が解読されたことにはならず、固定の鍵をしようする場合に比べて安全性は増す。また、復号時に複数の鍵を生成する際に暗号化に使用した鍵を計算するが、その鍵又はその鍵のシードを別に記憶しておく必要があるが、この方法ではその記憶量が複数個の鍵の個数に比例して大きくなるという欠点がある。ここで「鍵のシード」とは鍵の生成の元になる情報を表している。

【００１８】

更に、暗号化に関しては特開平９－１０７５３６号公報に記載されているように、ブロック連鎖法における暗号化処理として、Ｐ（１）を暗号鍵Ｋ及び初期値ＩＶに依存させて、暗号化関数Ｅ１を用いて暗号化し、Ｐ（ｉ）（２≦ｉ≦ｎ）は、暗号鍵Ｋ及びＰ（i-１）に依存させて、暗号化関数Ｅ２を用いて順次暗号化し、暗号化されたデータブロック（Ｃ（１），Ｃ（２），…，Ｃ（ｎ））を生成する方法が開示されている。しかしながら、この場合には、暗号鍵Ｋが固定であり、暗号化の基になるデータが暗号化を行うデータの前のデータであるため、暗号化が解かれる危険性が高いという問題があった。

【００１９】

【課題を解決するための手段】

上述した課題を解決するために、複数の単位ブロックが連続した情報を単位ブロック毎に暗号化する暗号化方法であって、所定の単位ブロックを暗号化するための暗号鍵のシードは、前記所定の単位ブロック以外の一つ又は複数の単位ブロック、もしくは、前記所定の単位ブロック以外の一つ又は複数の単位ブロックを暗号化した情報に基づくものであることを特徴とする暗号化方法を提供する。

【００２０】

また、再生順序のある複数の単位ブロックが連続した情報を単位ブロック毎に

暗号化する暗号化方法であって、所定の単位ブロックを暗号化するための暗号鍵のシードは、前記再生順序にて前記所定の単位ブロックより前の一つ又は複数の単位ブロック、もしくは、前記所定の単位ブロックより前の一つ又は複数の単位ブロックを暗号化した情報に基づくものであることを特徴とする暗号化方法を提供する。

【００２１】

更に、前記暗号鍵のシードが少なくとも２回以上連鎖していること特徴とする請求項２に記載の暗号化方法を提供する。

【００２２】

また、前記連鎖が所定の回数でリセットされることを特徴とする請求項３に記載の暗号化方法を提供する。

【００２３】

【発明の実施の形態】

以下、本発明に係る暗号化方法の一実施例について図面を参照して説明する。デジタルコンテンツデータが放送局から送られてくるＡＶデータであり、「コピー禁止」である場合、放送が行われた時間帯以降の任意の時間にその番組を一回だけ視聴できる記録再生装置としてハードディスクレコーダーを例に説明する。

【００２４】

本実施例では、「コピー禁止」のコンテンツについて、一回のみ視聴可能とすることでこのようなハードディスクレコーダーを実現している。ハードディスクにはＭＰＥＧ（Motion Picture Expert Group）のトランスポートストリーム（ＴＳ）を記録する。なお、暗号化／復号化にはＤＥＳを使用する。

【００２５】

図４は本発明に係る暗号化方法を適用した暗号化部を内蔵したハードディスクレコーダーの記録部を示す図である。チューナー１や外部信号入力部２によってＭＰＥＧのＴＳが入力されて、スイッチ回路部３へ送られる。ここでユーザーインターフェース２００によって出された指示に従って、チューナー１又は外部信号入力部２から記録信号処理部４に信号が送られる。記録信号処理部４に送られた信号に対してそこでタイムコード、絶対トラック番号などが生成される。その

後、信号は暗号化部５に送られてデータの暗号化が行われる。そして、記録部６においてディスク１００に記録される。なお、ディスク１００には、映像信号、音声信号の他にタイムコードなどが例えばサブコードエリアに記録される。

【００２６】

また、図５は本発明に係る暗号化方法によって暗号化された信号を復号化する復号化装置を内蔵したハードディスクレコーダーの再生部を示す図である。まず、再生部１０によってディスク１００の信号を読み取り、読み取った信号は復号化部９に送られる。そこでデータの復号化が行われた後、再生信号処理部８に送られ、エラー訂正等が行われた後、外部信号出力部７を介してモニタ３００に出力される。

【００２７】

このように図４及び図５に示す構成のハードディスクレコーダーにおいて、「コピー禁止」のデジタルコンテンツデータを記録する場合には、「コピー禁止」を示す信号を前述したＣＧＭＳによって記録する。例えば、デジタル放送では、ＴＳにdigital copy control descriptorという記述子があり、更にその中にdigital recording control data（デジタルコピー制御情報）という２ビットのフィールドがある。そのフィールドの中に例えば「コピー可」＝００、「一回コピー可」＝１０、コピー禁止」＝１１というように記述される。入力された信号に対して、ハードディスクレコーダーが「１１」という２ビットを検知すると、同一コンテンツでは一定の$Const_i$を初期ベクトル生成関数h_iの入力として初期値$IV=h_i(Const_i)$を計算する。

【００２８】

初期値ＩＶは、入力されたコンテンツの最初の単位ブロックを暗号化する際の鍵のシードとなるものである。従って初期値ＩＶが簡単に知られてしまうと暗号化されたコンテンツが解読される恐れがあるので、初期値ＩＶはハードディスク外の解析が困難な媒体に記録する。媒体としては、例えば、取り外しが困難なフラッシュメモリー等を使用する。この場合、単位ブロックを１８４バイトとして考えると、初期値ＩＶを鍵生成関数ｇの入力として鍵$K_1=g(IV, Const)$を計算する。以後、K_iは、ｉ番目のブロックを暗号化／復号化する際に使

う鍵を表すものとする。また、Ｃｏｎｓｔは鍵生成の元になるその他の情報を表すものとする。ここで、Ｃｏｎｓｔの情報が同一コンテンツ内で時間と共に変化するものと仮定すると、Ｃｏｎｓｔの情報を記憶しておかなければならない。また、それらの情報が時間と共に変化するものである場合、変化した全ての情報を記憶しておくための大容量のフラッシュメモリーを使用しなければならなくなるので、Ｃｏｎｓｔは例えばハードディスク固有のＩＤなど同一のコンテンツ内で一定のパラメータからなるものとする。なお、暗号化／復号化にはＤＥＳを使用しているので、鍵K_iが５６ビットである必要がある。よって、初期値ＩＶとＣｏｎｓｔとのビット数の合計が５６ビット以上になる方が好ましい。なぜならば、鍵生成関数ｇが１対１関数であると鍵K_iから初期値ＩＶやＣｏｎｓｔが推測し易くなるからである。従って、鍵生成関数ｇがｎ（ｎ≧２）対１関数となるようにする。

【００２９】

次に図６を用いて本発明に係る暗号化方法について説明する。１ＴＳパケットの１８８バイトのうち、ヘッダの４バイトを除いた単位ブロックの１８４バイトという値は、ＡＶデータが記録されている領域のバイト数である。ＴＳパケットＰ（１）のＡＶデータである１８４バイトの中にＤＥＳの暗号化ブロック６４ビットが２３ブロック分ある。そして、この２３ブロックに対してそれぞれＴＳパケットＰ（１）の暗号化鍵K_1で暗号化する。なお、暗号化されたＰ（１）はＣ（１）と記載する。なお、ＴＳパケットＰ（２），Ｐ（３），…に関しても同様の操作を行う。

【００３０】

次に、Ｐ（２）の暗号化に使用する鍵K_2の作成方法を説明する。鍵K_2＝ｇ（S_1，Ｃｏｎｓｔ）と定義する。ここで、S_1とは鍵シード生成関数をｈとするとS_i＝ｈ（Ｐ（ｉ））で定義されるものとする。すなわち、一つ前の単位ブロックの平文を鍵のシードとする。これによって鍵は１単位ブロック毎に可変になり、たとえ一つの鍵が分かっても全ての平文を解読するのは困難である。また、このほかにも鍵のシードを複数用意することによって鍵を可変にする方法があるが、全ての鍵のシードを別に記憶しておく必要があった。しかし、本発明の方法を採

用すると、鍵のシードの可変部分はハードディスク上に記録している暗号文を復号化した平文であるから、解析することも困難で別の領域に記憶しておく必要もない。K_3以降もK_3＝ｇ（S_2，Ｃｏｎｓｔ），K_4＝ｇ（S_3，Ｃｏｎｓｔ），…となる。

【００３１】

一方、再生する際にはフラッシュメモリー上の初期値ＩＶを読んで鍵K_1を生成し、Ｐ（１）を暗号化する。その際、Ｐ（１）からS_1も同時に生成しておく。次に、そのS_1から鍵K_2を生成し、Ｐ（２）を暗号化する。暗号化と復号化の概略を図７に示す。また、上述した実施例では、一つ前の単位ブロックから暗号鍵のシードを生成していたが、単位ブロックの暗号鍵のシードを過去の一つの単位ブロックから生成しても良く、例えば二つ前の単位ブロックを使用しても良い。

【００３２】

次に、「コピー禁止」のコンテンツを途中まで再生したときに、一度再生した部分が見られないようにする方法について説明する。図８に示すようにＴＳパケットＣ（１）からＣ（４）までを再生するものとする。上述した説明のように、まず初期値ＩＶを読んでＣ（１）から復号化を開始する。そして、Ｃ（４）の復号化を終了した時点で再生を終了する。ここで、次回にＣ（１）からＣ（４）までのデータを再生できないようにするために、フラッシュメモリーに記録されていた初期値ＩＶを消去する。これによってＣ（１）を復号化するための鍵K_1を生成することができなくなる。しかし、次回、Ｃ（５）から再生を開始するためにはＣ（５）を復号するための鍵K_5のシードS_4を記録しておかなければならない。従って、再生を開始した時点で初期値ＩＶをフラッシュメモリーから消去、又は、その後必要な場合はバッファに移動する。そして、再生を終了した時点でS_4をフラッシュメモリーに記録する。これにより、次回はＣ（１）からＣ（４）が復号できないことにより再生ができなくなる。一方、フラッシュメモリーにS_4と共にＰ（５）の先頭アドレス等を記録しておくことによって次回からＣ（５）以降の再生が可能になる。この例では、S_iはＣ（ｉ＋１）の復号化に使用する鍵K_{i+1}のシードとなっているが、二つの初期値IV_1とIV_2とを持つこと

によってS_iをＣ（ｉ＋２）の復号化に使用する鍵K_{i+2}のシードにしても良い。同様に、初期値ＩＶを３つ、４つ、…と持つことによって、S_iを３つ、４つ先の単位ブロックを復号化するためのシードとして使用可能である。また、K_{i+2}のシードをS_iとS_{i+1}のように複数にする、すなわち過去の二つ以上の平文を元に鍵を生成しても良い。このようにS_iがK_{i+1}、S_{i+1}がK_{i+2}、…のシードになっていることを以後、「連鎖している」と呼ぶこととする。

【００３３】

元々、「コピー禁止」のコンテンツは放送時に一度だけ視聴することができるという趣旨で放送されているものである。従って、一度再生した部分を巻戻して視聴するのは著作権者の意図に反する可能性が高いので許可されないことがある。しかし、現行の「コピー禁止」のコンテンツは巻戻して視聴することができないのは当然であるが、途中から視聴することは可能である。よって、「コピー禁止」のコンテンツをハードディスクレコーダーに記録して、早送りのみは許可される可能性はある。そこで、上述した方法で早送りを行うと、ランダムアクセスに優れたハードディスクであるにもかかわらず、必ずＣ（１）から復号していかなければならない。従って、コンテンツの後半の方から視聴するようなことがあると、そこまでアクセスするのに非常に時間がかかってしまう。そこで、以下のような構成が考えられる。

【００３４】

図９にその概略を示す。図中の矢印は矢印の始点にある情報が指している情報を暗号化するための鍵のシードになることを示す。隣のブロックの連鎖をこまめにリセットして、その代わりにリセットがかかった次にＰ（２－１）というブロックを設ける。Ｐ（２－１）は、初期値ＩＶをシードにした鍵で暗号化される。そして、Ｐ（２－１）はＰ（２－２）とＰ（３－１）の暗号化鍵のシードとなる。このような構成により、例えばＰ（３－４）にアクセスしたい場合は、初期値ＩＶ→Ｐ（２－１）→Ｐ（３－１）→Ｐ（３－２）→Ｐ（３－３）→Ｐ（３－４）という順序で復号化していけば短い時間でアクセスすることが可能となる。このような構成を以後二つの「階層」と呼ぶことにする。そして、Ｐ（２－１），Ｐ（３－１），Ｐ（４－１），…のことを「第２階層」と呼ぶことにする。なお

、上述した実施例では、この階層の数が二つの場合を説明したが、階層の数を三つ以上にしても良い。しかし、階層の数を三つ以上にするとランダムアクセスにかかる時間が短縮されるという利点があるものの、暗号化／復号化の方法が複雑になるという欠点がある。なお、ここからは、第１階層の単位ブロックを暗号化／復号化する鍵のシードを生成する関数をh_1、第２階層の単位ブロックを暗号化／復号化する鍵のシードを生成する関数をh_2、…と記述する。また、第２階層のＰ（２－１）によって生成される鍵K_{3-1}のシードをT_{2-1}、Ｐ（３－１）によって生成される鍵K_{4-1}のシードをT_{3-1}、…とする。

【００３５】

次に、複数の階層になっている場合に、コンテンツの一度再生した部分を視聴不可能とする方法について説明する。図１０に示すように、ＴＳパケットＣ（１－１）からＣ（２－３）までを再生するものとする。再生開始時には、フラッシュメモリーには初期値ＩＶが記録されている。そして、再生を開始した時点で初期値ＩＶをフラッシュメモリーから消去、又は、その後必要なときにはバッファに移動して、Ｃ（２－３）まで再生が終了した時点でT_{2-1}とS_{2-3}をフラッシュメモリーに記録する。S_{2-3}を記録する理由は複数の階層を持たなかったときと同様にK_{2-4}を生成するため、すなわちＣ（２－４）から再生できるようにするためである。一方、Ｃ（２－３）まで再生を終了して、次回、Ｃ（４－１）から再生したい場合には、第２階層のＣ（４－１）にできるだけ速くランダムアクセスするために、T_{2-1}→Ｃ（３－１）→Ｃ（４－１）と進むのが最も速い。従って、ランダムアクセスのためにT_{2-1}もフラッシュメモリーに記録している。更に、Ｃ（２－４）からの再生とランダムアクセスが可能になる。

【００３６】

以上、ハードディスクレコーダーで「コピー禁止」のデジタルコンテンツを記録する際の説明を行ってきた。なお、本実施例ではＭＰＥＧのＴＳパケットのデジタルコンテンツデータに相当する１８４バイトを単位ブロックのサイズとして取ってきたが、これはアプリケーションに応じてさまざまなサイズを取ることが可能である。図７や図９のような連鎖を一つのコンテンツを通して行った場合、途中でデータを誤って読み取ったり、誤って記録したりすることで正しく再生で

きなくなることがある。この場合、一箇所の誤りがその後も連鎖するために起きるものなので、これを防止するために初期値ＩＶから始まる連鎖を同一コンテンツ内で複数回リセットするという方法を取ることもできる。例えば図１１に示すように初期値ＩＶを複数用意することによって連鎖が複数回リセットされることになるので、誤りの伝播を防止することができる。

【００３７】

なお、本実施例ではハードディスクレコーダーについてのみ説明してきたが、「コピー禁止」のコンテンツの場合には、光ディスクレコーダーなどでも実現可能であるし、ランダムアクセスができなくなるが、コンテンツを最初から再生する場合にはテープレコーダーでも実現可能である。

【００３８】

これまでは「コピー禁止」のコンテンツの場合について説明してきたが、以下、放送局から送られてくるデジタルコンテンツデータが「一回コピー可」である場合に、その番組を一つの別媒体にのみ記録することができる記録再生装置の例としてハードディスクレコーダーとデジタルＶＴＲを組み合わせた記録再生装置について説明する。本発明の実施の形態では、「一回コピー可」のコンテンツについては、一回のみ別媒体に記録可能とすることで、このようなハードディスクレコーダーとデジタルＶＴＲとを組み合わせた記録再生装置を実現した。ハードディスクレコーダーのハードディスクとＶＴＲのビデオテープにはＭＰＥＧのＴＳを記録する。そして、暗号化／復号化にはＤＥＳを使用する。

【００３９】

図１２は、本発明の一実施例であるハードディスクレコーダーとデジタルＶＴＲとを組み合わせた記録再生装置の記録部のブロック図である。同図において、チューナー１や外部信号入力部２によってＭＰＥＧのＴＳパケットが入力されて、スイッチ回路部３に送られる。ここで、ユーザーインターフェース２００から出された指示に従って、テープ記録信号処理部１２又はディスク記録信号処理部１４に信号が送られる。テープ記録信号処理部１２に送られた信号に対してはタイムコードや絶対トラック番号等が生成される。その後、テープ記録部１３に送られてテープ３００にデジタル記録される。テープ３００には映像信号、音声信

号の他にタイムコード、絶対トラック番号等が例えばサブコードエリアに記録される。また、ディスク記録信号処理部１４に送られた信号に対してタイムコード等が生成される。その後、ディスク記録部１５に送られてディスク１００にデジタル記録される。そして、ハードディスクにもテープ同様に映像信号、音声信号の他にタイムコードや絶対トラック番号等が記録される。ディスク再生信号処理部１７は、ハードディスクレコーダーにて記録された信号を再生するもので、この再生信号をテープ記録信号処理部１２へ送ることでデータのコピーを行うことができる。

【００４０】

図１３は本発明におけるデジタル信号記録再生装置の再生部のブロック図である。テープ再生時には、テープ再生部１９によってテープ３００の信号を読み取る。そして、その信号はテープ再生信号処理部１８に送られ、そこでエラー訂正等が行われた後、スイッチ回路部３に送られる。また、ディスク再生時には、ディスク再生部２１によってディスク１００の信号を読み取る。そして、その信号はディスク再生信号処理部２０に送られ、そこでエラー訂正等が行われた後、スイッチ回路部３とテープ記録信号処理部１７へ送られる。そして、ユーザーインターフェース２００によって出された指示に従って、テープ３００の再生信号又はディスク１００の再生信号を外部信号出力部１６を介してモニタ４００に出力する。

【００４１】

次に、図１２、図１３に示す構成のハードディスクレコーダーとデジタルＶＴＲとを組み合わせた記録再生装置によって、「一回コピー可」のデジタルコンテンツデータを記録する際の説明を行う。「一回コピー可」を示す信号は、「コピー禁止」を示す信号と同様にＣＧＭＳによって記録される。例えば、デジタル放送ではＴＳにdigital copy control descriptorという記述子があり、更にその中にdigital recording control data（デジタルコピー制御情報）という２ビットのフィールドがある。そのフィールド中で例えば「コピー可」＝００、「一回コピー可」＝１０、「コピー禁止」＝１１というように記述される。入力された信号に対して、記録再生装置がその「１０」という２ビットを検知すると

、同一コンテンツでは一定のＣｏｎｓｔ$_i$を初期ベクトル生成関数ｈ$_i$の入力とし、初期値ＩＶ＝ｈ$_i$（Ｃｏｎｓｔ$_i$）として計算する。以下、「コピー禁止」の場合と同様に暗号化を行う。また、「一回コピー可」のコンテンツは「コピー禁止」のコンテンツと異なり、再生に関しては何度行っても良いので、「一回コピー可」のコンテンツは別媒体に記録を行う際に限って鍵を消去することとする。例えば、図８に示すように、ハードディスクに記録されたＣ（１）からＣ（４）までをテープに記録し始めたらフラッシュメモリーから初期値ＩＶを消去して、Ｃ（４）までの記録が終了したらシードＳ$_4$をフラッシュメモリーに記録する。従って、再生の際には、フラッシュメモリーの初期値ＩＶは参照をするが、フラッシュメモリーに対しての記録や消去は行わない。

【００４２】

また、「コピー禁止」のコンテンツに関しては、元々デジタル放送のＰＰＶのコンテンツが一回のみ視聴可能という意図で放送されているので、途中の単位ブロックから再生した場合、それ以前のデータの再生は許可されず、そのことは考慮する必要がなかった。しかしながら、視聴者が所望の部分だけをコピーしたり、一つのコンテンツを分割して複数のテープにコピーすることもできる。例えば、図１４に示すように、Ｃ（２－３）以降をテープにコピーして、それ以前はハードディスク上で再生できるようにしておくこともできる。その方法としては、まずＣ（２－３）からテープにコピーを開始し、単位ブロックＣ（２－３）をコピーし終えた時点でＣ（２－３）のデータ自体を消去するかＣ（２－３）のデータを関係のないデータに書き換える。そして、フラッシュメモリーのデータの書き換えは行わない。これによって、コピーが終了するとＣ（２－３）はデータ自体が存在しないので復号化はできず、同時にＫ$_{2-4}$も生成することができない。しかし、初期値ＩＶとＣ（２－１）が残っていることにより初期値ＩＶ→Ｃ（２－１）→Ｃ（３－１）→ということでＣ（３－１）以降は復号化が可能になる。従って、これを避けるためにＣ（３－１）までコピーが終了した時点でＣ（２－３）と同様にＣ（３－１）も消去する。これでＣ（３－２）以降は再生が不可能になる。また、例えばＣ（２－３）からＣ（３－３）までコピーする場合は、上述したものを組み合わせることによってＣ（２－３）とＣ（３－１）を消してＴ

S_{3-1}とS_{3-3}とをフラッシュメモリーに記録すれば良い。

【００４３】

以上、ハードディスクレコーダーとデジタルＶＴＲとを組み合わせた記録再生装置で「一回コピー可」のデジタルコンテンツを記録する際の説明を行った。なお、ハードディスクレコーダーとデジタルＶＴＲとを組み合わせた記録再生装置についてのみ説明してきたが、「一回コピー可」のコンテンツの場合、ハードディスクドライブ部には光ディスクレコーダー等のランダムアクセスが可能な記録装置であれば置換可能であり、ＶＴＲ部にはあらゆる記録装置で置換可能である。

【００４４】

【発明の効果】

以上、詳述したように、本発明に係る暗号化方法によれば、「コピー禁止」のコンテンツについて、今までは放送時のみしか視聴することができなかったが、視聴者が視聴したい時間にコンテンツを一度のみ視聴することが可能となった。また、「一回コピー可」のコンテンツも、媒体に記録した後で一度限り別の媒体にコピー及び編集することが可能となる。そして、その際にハードディスク上にあるデータのセキュリティに関しては暗号化されることによって保障される。更に、「コピー禁止」のコンテンツに対して途中までコンテンツを見た場合には、それまでの復号化鍵のシードを消去する方法によって途中の地点までの再生を不可能にするという機能も実現可能である。同様に、「一回コピー可」のコンテンツも別の媒体にコピーした部分は再生を不可能とすることができる。また、暗号鍵のシードが所定の単位ブロック以外の平文、もしくは、暗号文であることによって、所望のブロック以降の再生を不可能にするという機能も実現可能である。そして、連鎖する方式を取ることにより、記録しておく鍵のシード情報の容量が非常に少なくて済む。

【図面の簡単な説明】

【図1】

ＤＥＳの基本構成を示す図である。

【図２】

ＤＥＳの基本単位である１６段の変換部の構造を示す図である。

【図３】

ＤＥＳで用いられる関数ｆの構造を示す図である。

【図４】

本発明に係る暗号化方法を適用したハードディスクレコーダーの記録部の構成を示すブロック図である。

【図５】

本発明に係る暗号化方法を適用して記録した信号を再生するハードディスクレコーダの再生部の構成を示すブロック図である。

【図６】

本発明に係る暗号化方法におけるＭＰＥＧのＴＳの構成と暗号化の概略を示す図である。

【図７】

本発明に係る暗号化方法による暗号化と復号化方法及び復号化装置による復号化を示す図である。

【図８】

本発明に係る暗号化方法によって暗号化されたコンテンツの再生方法を示す図である。

【図９】

本発明に係る暗号化方法による暗号化の一例を示す図である。

【図１０】

本発明に係る暗号化方法によって暗号化されたコンテンツの別の再生方法を示す図である。

【図１１】

本発明に係る暗号化方法による暗号化の別の例を示す図である。

【図１２】

本発明に係る暗号化方法を適用したハードディスクレコーダーとデジタルＶＴＲとを組み合わせた記録再生装置の記録部を示すブロック図である。

【図１３】

本発明に係る暗号化方法を適用したハードディスクレコーダーとデジタルＶＴＲとを組み合わせた記録再生装置の再生部を示すブロック図である。

【図１４】

本発明に係る暗号化方法を適用したハードディスクレコーダーとデジタルＶＴＲとを組み合わせた記録再生装置の再生方法を示す図である。

【符号の説明】

１　チューナー

２　外部信号入力部

３　スイッチ回路部

４　記録信号処理部

５　暗号化部

６　記録部

７　外部信号出力部

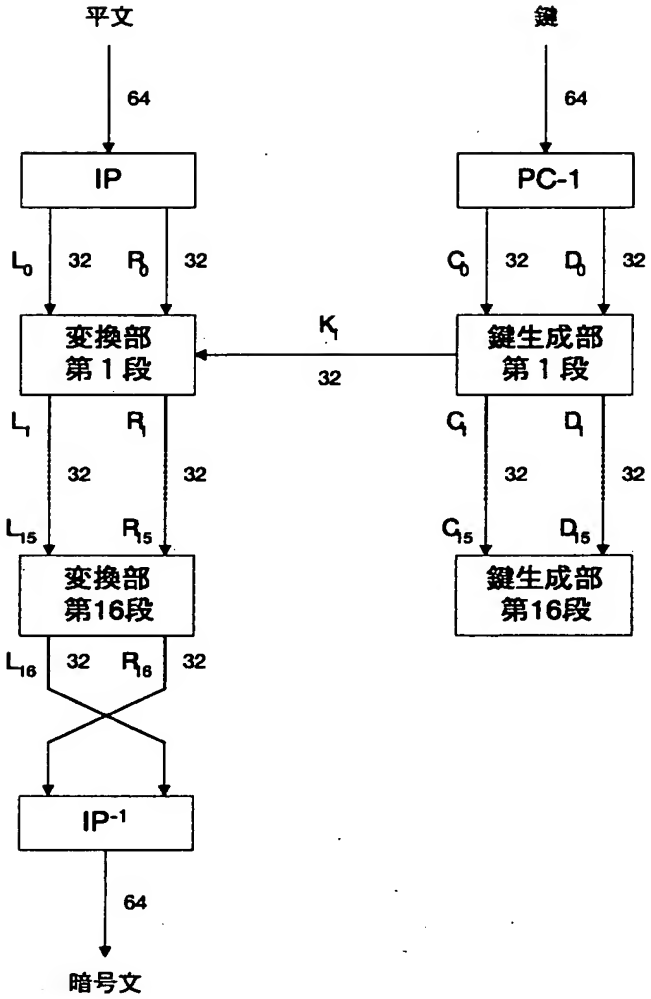
８　再生信号処理部

９　復号化部

１０　再生部

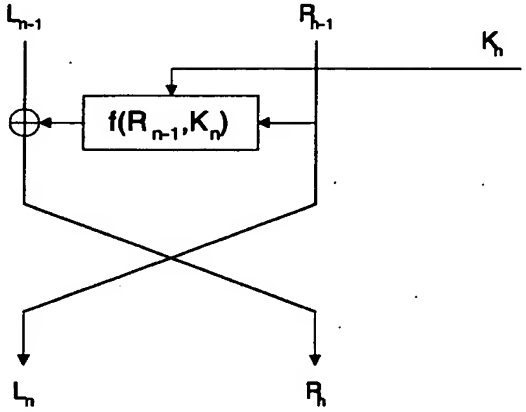
【書類名】　　図面

【図１】

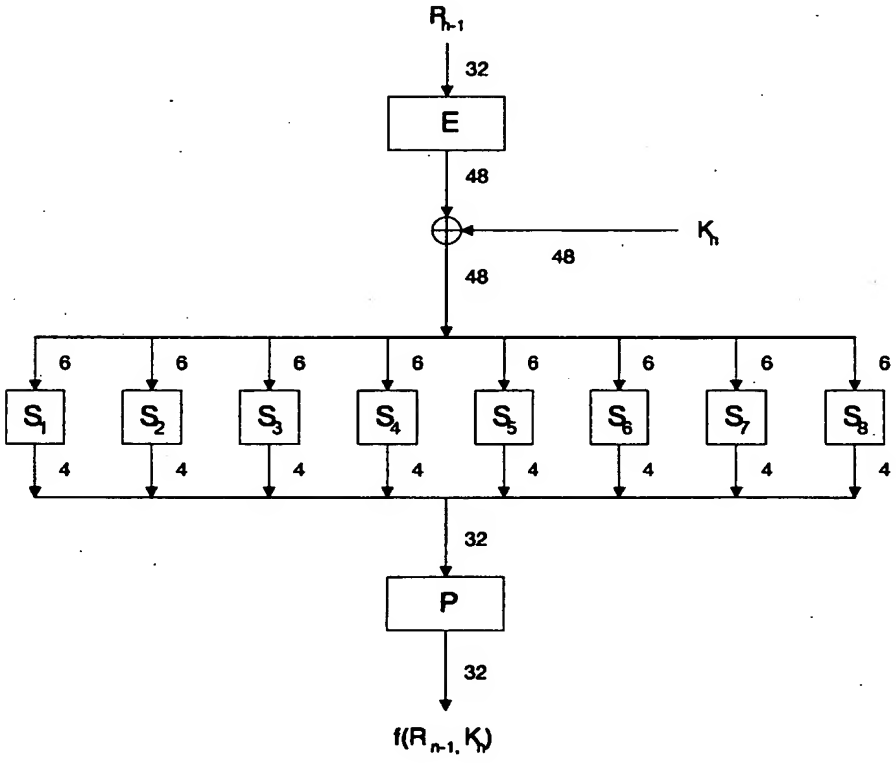


出証特２００１－３１１２８７９

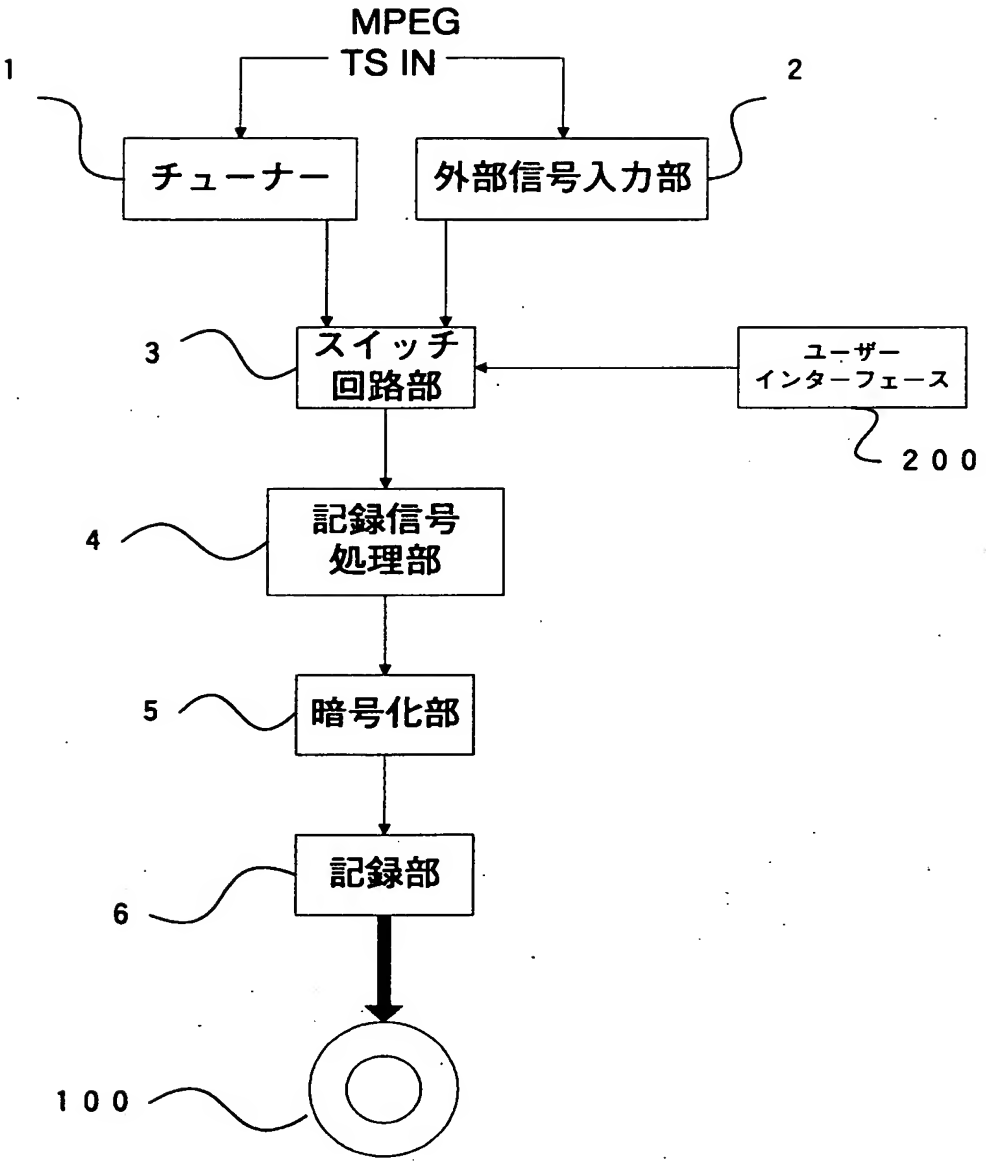
【図２】


L_{n-1}
R_{n-1}
K_n
$f(R_{n-1},K_n)$
L_n
R_n

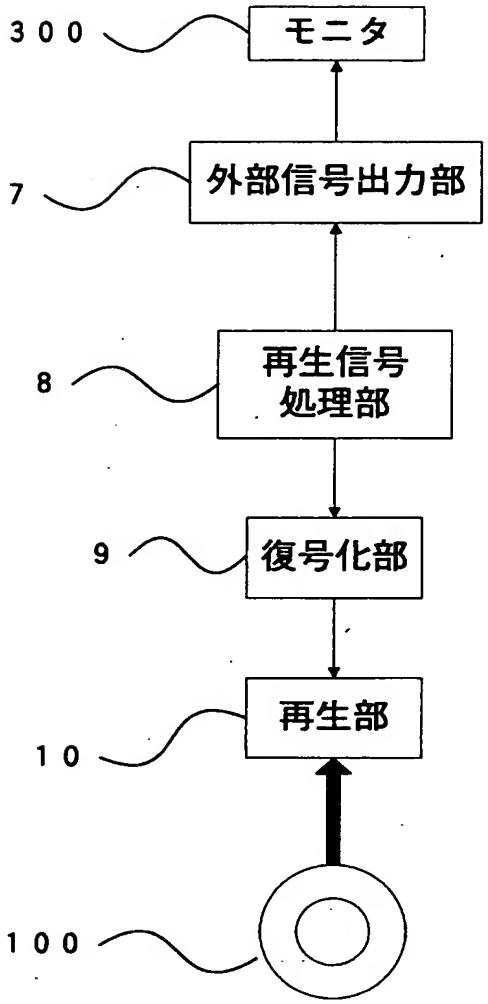
【図３】


R_{n-1}
32
E
48
K_n
48
48
6
S_1
S_2
S_3
S_4
S_5
S_6
S_7
S_8
4
32
P
32
$f(R_{n-1}, K_n)$

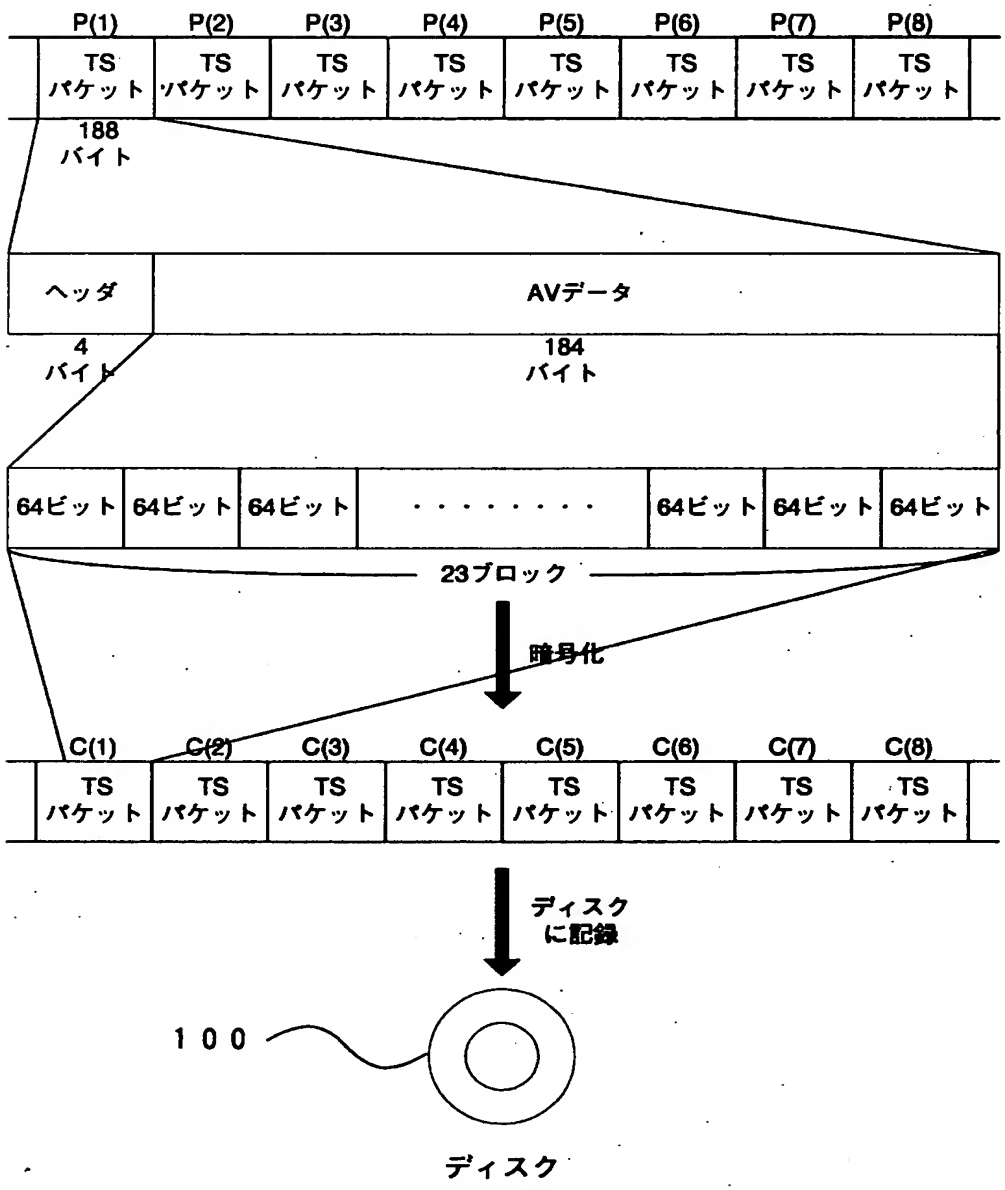
【図４】


MPEG
TS IN
1
2
チューナー
外部信号入力部
3
スイッチ
回路部
ユーザー
インターフェース
200
4
記録信号
処理部
5
暗号化部
記録部
6
100
ディスク

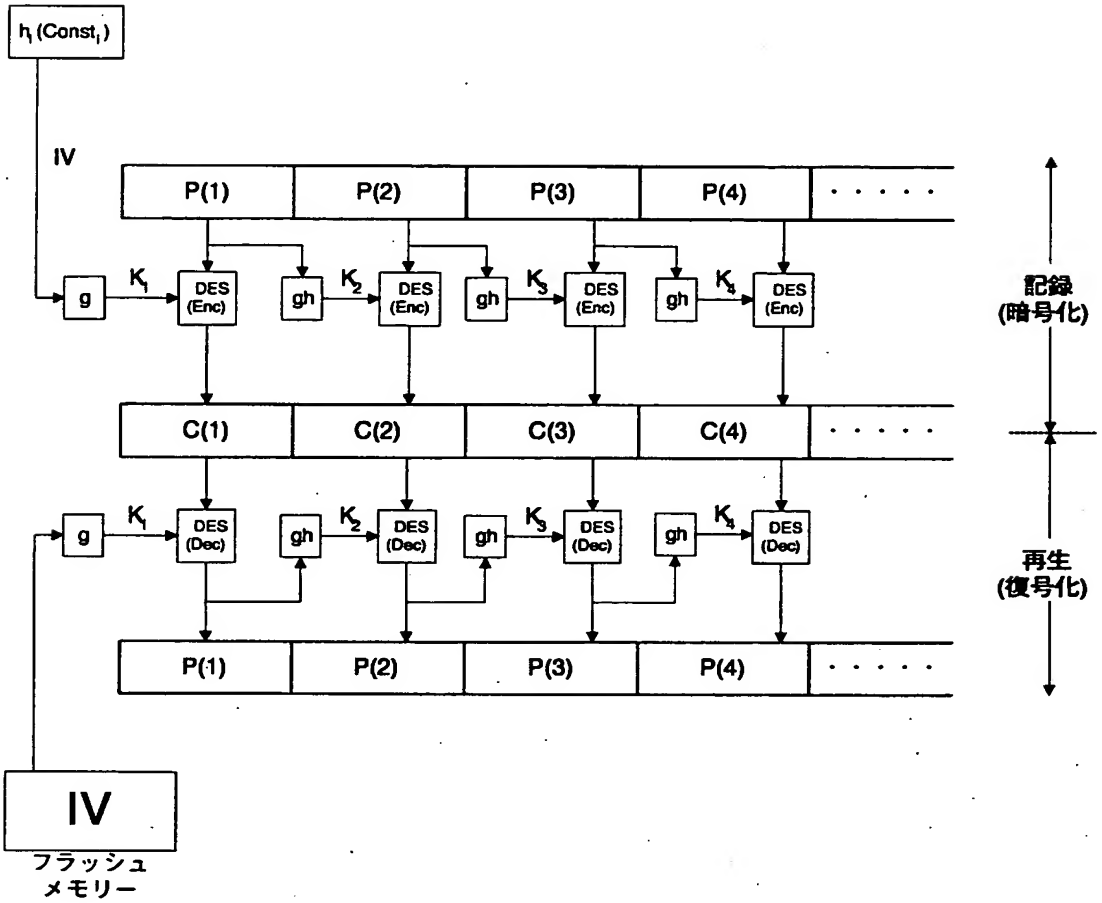
【図５】



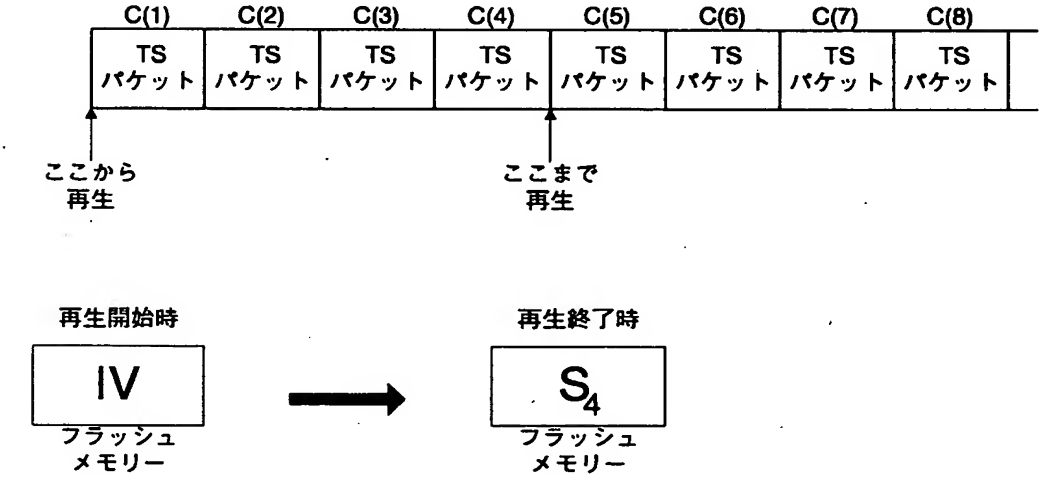
【図６】


P(1)
P(2)
P(3)
P(4)
P(5)
P(6)
P(7)
P(8)
TS パケット
188 バイト
ヘッダ
AVデータ
4 バイト
184 バイト
64ビット
64ビット
64ビット
・・・・・・・・
64ビット
64ビット
64ビット
23ブロック
暗号化
C(1)
C(2)
C(3)
C(4)
C(5)
C(6)
C(7)
C(8)
ディスク に記録
１００
ディスク

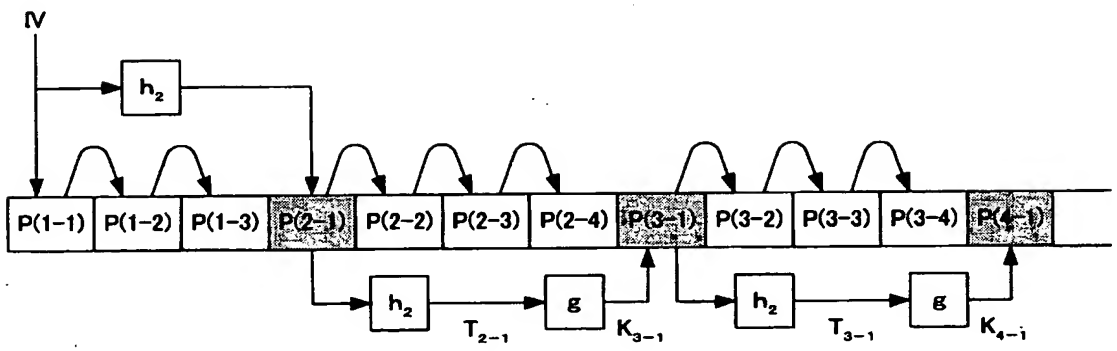
【図７】


h1(Const1)
IV
P(1)
P(2)
P(3)
P(4)
g
K1
DES (Enc)
gh
K2
K3
K4
C(1)
C(2)
C(3)
C(4)
DES (Dec)
記録 (暗号化)
再生 (復号化)
IV
フラッシュ メモリー

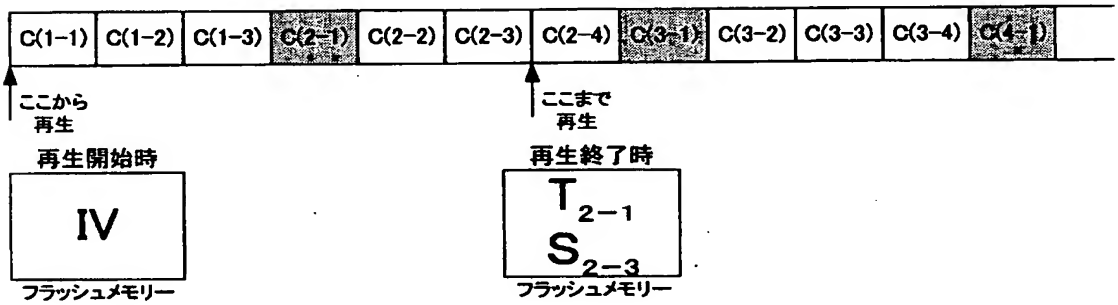
【図８】


C(1)
C(2)
C(3)
C(4)
C(5)
C(6)
C(7)
C(8)
TS パケット
ここから 再生
ここまで 再生
再生開始時
再生終了時
IV
S4
フラッシュ メモリー

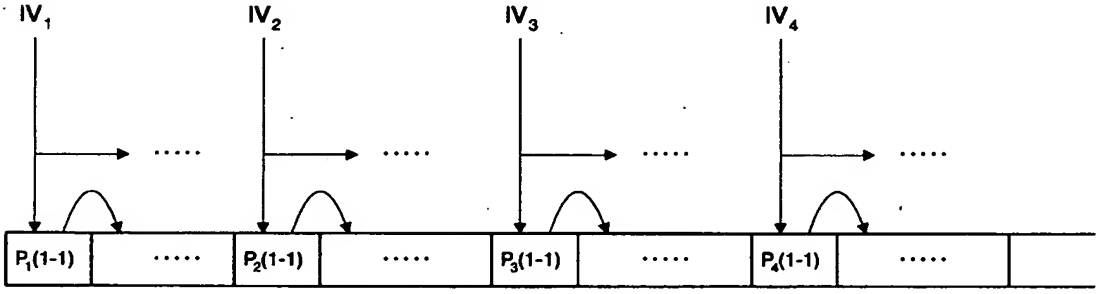
【図９】


IV
h2
P(1-1)
P(1-2)
P(1-3)
P(2-1)
P(2-2)
P(2-3)
P(2-4)
P(3-1)
P(3-2)
P(3-3)
P(3-4)
P(4-1)
h2
T2-1
g
K3-1
h2
T3-1
g
K4-1

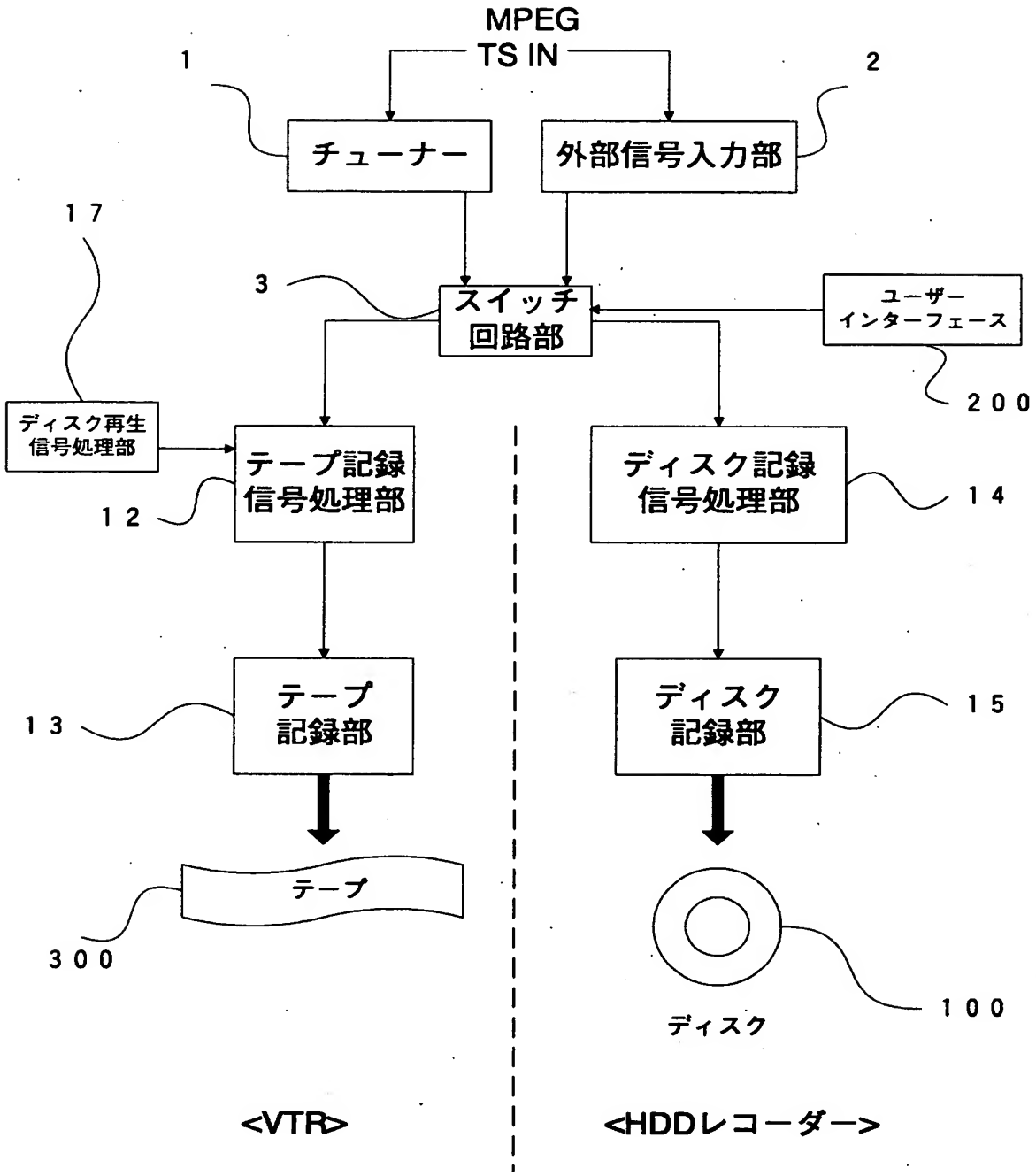
【図１０】


C(1-1)
C(1-2)
C(1-3)
C(2-1)
C(2-2)
C(2-3)
C(2-4)
C(3-1)
C(3-2)
C(3-3)
C(3-4)
C(4-1)
ここから再生
ここまで再生
再生開始時
IV
フラッシュメモリー
再生終了時
T2-1
S2-3
フラッシュメモリー

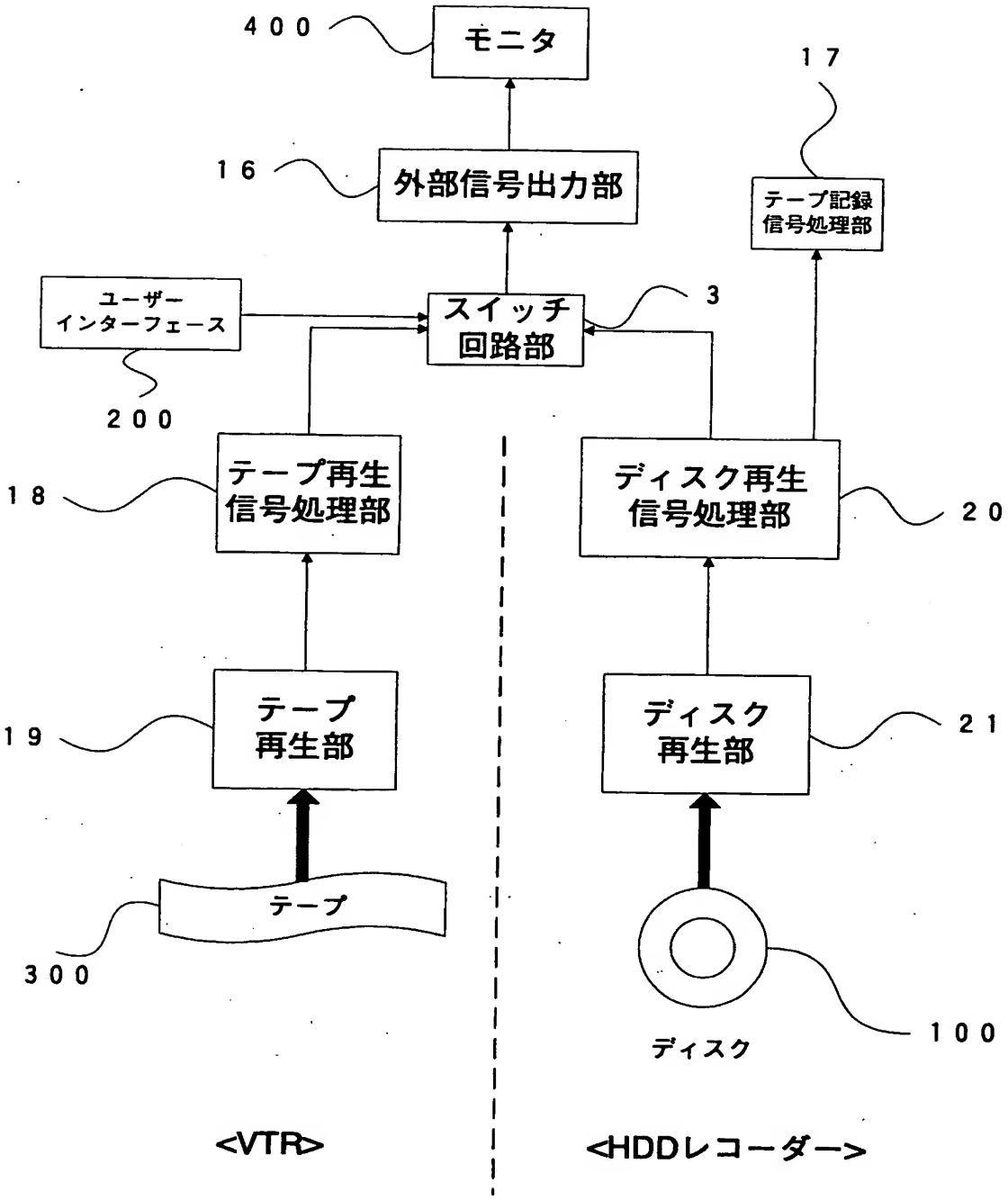
【図１１】


IV1
IV2
IV3
IV4
P1(1-1)
P2(1-1)
P3(1-1)
P4(1-1)

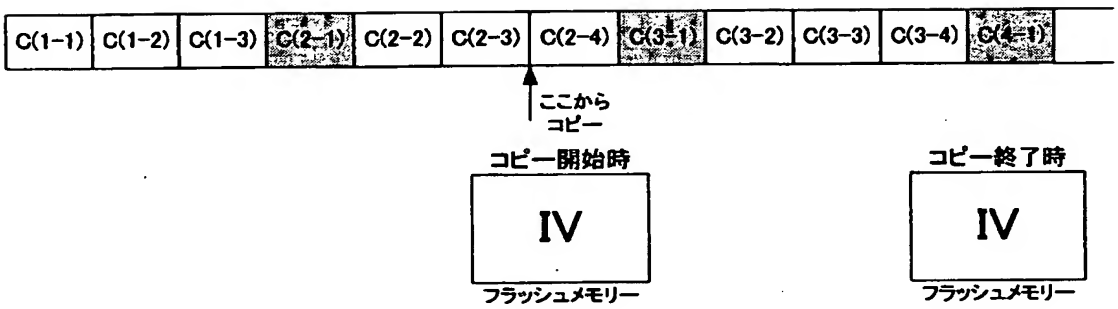
【図１２】


MPEG
TS IN
1
2
チューナー
外部信号入力部
17
3
スイッチ
回路部
ユーザー
インターフェース
200
ディスク再生
信号処理部
テープ記録
信号処理部
12
ディスク記録
信号処理部
14
テープ
記録部
13
ディスク
記録部
15
テープ
300
ディスク
100
<VTR>
<HDDレコーダー>

【図１３】


４００
モニタ
１７
１６
外部信号出力部
テープ記録
信号処理部
ユーザー
インターフェース
スイッチ
回路部
３
２００
テープ再生
信号処理部
１８
ディスク再生
信号処理部
２０
テープ
再生部
１９
ディスク
再生部
２１
テープ
３００
ディスク
１００
<VTR>
<HDDレコーダー>

【図１４】


C(1-1)
C(1-2)
C(1-3)
C(2-1)
C(2-2)
C(2-3)
C(2-4)
C(3-1)
C(3-2)
C(3-3)
C(3-4)
C(4-1)
ここから
コピー
コピー開始時
IV
フラッシュメモリー
コピー終了時
IV
フラッシュメモリー

【書類名】　　要約書

【要約】

【課題】　　「コピー禁止」のコンテンツについて、視聴者が視聴したい時間にコンテンツを一度のみ視聴することを可能とし、また、「一回コピー可」のコンテンツについて、媒体に記録した後で一度限り別の媒体にコピー及び編集することを可能とすると共に、その際にデータのセキュリティを保障する。

【解決手段】　複数の単位ブロックが連続した情報を単位ブロック毎に暗号化する暗号化方法であって、所定の単位ブロックを暗号化するための暗号鍵のシードは、前記所定の単位ブロック以外の一つ又は複数の単位ブロックの暗号文若しくは平文を基にした情報である。

【選択図】　　図７

出　願　人　履　歴　情　報

識別番号　　〔０００００４３２９〕

１．変更年月日　　１９９０年　８月　８日
［変更理由］　新規登録
住　所　神奈川県横浜市神奈川区守屋町３丁目１２番地
氏　名　日本ビクター株式会社